

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Satoshi ANDO et al. :
Serial No. NEW : **Attn: APPLICATION BRANCH**
Filed March 26, 2004 : Attorney Docket No. 2004-0466A

ACCESS-CONTROLLING METHOD,
REPEATER, AND SERVER

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2003-103760, filed April 8, 2003, as acknowledged in the Declaration of this application.

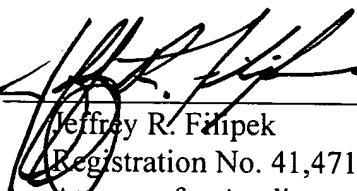
A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Satoshi ANDO et al.

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

By



Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/kes
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
March 26, 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 4月 8日
Date of Application:

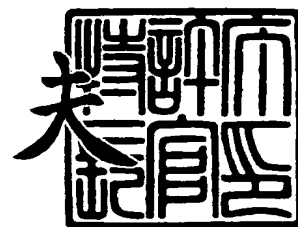
出願番号 特願2003-103760
Application Number:
[ST. 10/C]: [JP 2003-103760]

出願人 松下電器産業株式会社
Applicant(s):

2004年 1月14日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3111542

【書類名】 特許願
【整理番号】 2022540383
【提出日】 平成15年 4月 8日
【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/26
H04L 12/46
H04L 12/56
G06F 13/00
G06F 15/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 安藤 智

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 川口 雄一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 大元 政雄

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 志水 郁二

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 大浦 正登

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097179

【弁理士】

【氏名又は名称】 平野 一幸

【手数料の表示】

【予納台帳番号】 058698

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0013529

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 アクセス制御方法、中継装置及びサーバ

【特許請求の範囲】

【請求項 1】 外部ネットワークの端末から内部ネットワークのサーバへのアクセスを、前記外部ネットワークと前記内部ネットワークとを中継する中継装置を介して、制御するアクセス制御方法であって、

前記端末が前記サーバ宛に送出するパケットの伝送を、一定条件下で許容する第 1 ステップと、

許容されたパケットに対し、前記サーバが接続を許可した場合、前記サーバ宛のパケット伝送の条件を変更する第 2 ステップと、

しかる後、変更された条件で、前記端末と前記サーバとのパケット伝送を制御する第 3 ステップとを含む、アクセス制御方法。

【請求項 2】 前記第 1 ステップにおける一定条件は、前記端末から前記サーバ宛のパケット伝送の帯域を、一定範囲内とするものである、請求項 1 記載のアクセス制御方法。

【請求項 3】 前記第 1 ステップにおいて許容されるパケットは、前記サーバへ送信される認証情報を含む、請求項 1 から 2 記載のアクセス制御方法。

【請求項 4】 前記第 2 ステップにおいて、前記端末と前記サーバとのそれぞれのアドレス及びポート番号に係る、フローについて、条件が変更される、請求項 1 から 3 記載のアクセス制御方法。

【請求項 5】 外部ネットワークの端末から内部ネットワークのサーバへのアクセスを、前記外部ネットワークと前記内部ネットワークとを中継する中継装置を介して、制御するアクセス制御方法であって、

前記端末から暗号化されたパケットが、前記サーバに到着した際、前記サーバは、この暗号化されたパケットを復号し、前記サーバは、前記中継装置に、この暗号化されたパケットに係る、アクセス制御に使用する情報を、前記中継装置へ通知する、アクセス制御方法。

【請求項 6】 アクセス制御に使用する情報には、暗号化されたパケットに係るフローを定義する情報が含まれる、請求項 5 記載のアクセス制御方法。

【請求項 7】 アクセス制御に使用する情報には、前記端末と前記サーバとのそれぞれのアドレス及びポート番号の情報が含まれる、請求項 5 から 6 記載のアクセス制御方法。

【請求項 8】 前記サーバと前記中継装置とのそれぞれにおいて、アクセス制御に使用する情報が保持され、前記サーバにおいて、この情報を変更した際、前記サーバは、その旨を前記中継装置へ通知する、請求項記載 1 から 7 記載のアクセス制御方法。

【請求項 9】 外部ネットワーク側に接続される第 1 の通信部と、
内部ネットワーク側に接続される第 2 の通信部と、
前記第 1 の通信部及び前記第 2 の通信部を介して伝送されるパケットに係るフローを定義する情報と、該当するフローについての帯域の閾値と、該当するフローについての帯域の測定値とを、関連付けて記憶する記憶部と、
前記記憶部に記憶されたフローを定義する情報にしたがって、パケットのフローを分類する分類部と、
分類されたフローについて帯域を測定し、測定値を前記記憶部に格納する測定部と、
分類されたフローについて、前記記憶部に格納された帯域の測定値と閾値とを大小比較し、伝送の許可を判定する判定部と、
前記判定部により伝送を許可されたパケットを、前記第 1 の通信部及び／又は前記第 2 の通信部を介して送信する帯域制御部とを備える中継装置。

【請求項 1 0】 前記記憶部における帯域の閾値は、内部ネットワークのサーバが、外部ネットワークの端末からの接続を許可するまで、接続を制限する値に設定され、内部ネットワークのサーバがこの接続を許可すると、より接続の制限を緩和する値に変更される、請求項 9 記載の中継装置。

【請求項 1 1】 内部ネットワーク側に接続される通信部と、
前記通信部を介して伝送されるパケットに係るフローを定義する情報と、該当するフローについての帯域の閾値と、該当するフローについての帯域の測定値とを、関連付けて記憶する記憶部と、
前記記憶部に記憶されたフローを定義する情報にしたがって、パケットのフロ

ーを分類する分類部と、

分類されたフローについて帯域を測定し、測定値を前記記憶部に格納する測定部と、

分類されたフローについて、前記記憶部に格納された帯域の測定値と閾値とを大小比較し、伝送の許否を判定する判定部と、

前記判定部により伝送を許可されたパケットを、前記通信部を介して送信する帯域制御部とを備えるサーバ。

【請求項 1 2】外部ネットワークの端末からの接続を許可するまで、前記記憶部における帯域の閾値を小さな値に設定し、この接続を許可すると、前記記憶部における帯域の閾値をより大きな値に変更する、請求項 1 1 記載のサーバ。

【請求項 1 3】前記記憶部に格納された情報を変更した際、その旨を中継装置へ通知する、請求項 1 1 から 1 2 記載のサーバ。

【請求項 1 4】暗号化されたパケットを復号する暗号処理部を備え、この暗号化されたパケットに係る、アクセス制御に使用する情報を、前記中継装置へ通知する、請求項 1 1 から 1 3 記載のサーバ。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、アクセス制御方法、中継装置、サーバに関するものである。

【0 0 0 2】

【従来の技術】

まず本明細書において、保護すべき情報又はそれを管理するサーバが存在する位置を、内部といい、この内部に対して、ネットワークを経由して通信する位置を、外部という。

【0 0 0 3】

さて、アクセス制御（ファイアーウォール、パケットフィルタリングとも呼ばれる）は、次のような不正アクセスから、内部を保護するために使用される。即ち、この不正アクセスとしては、外部から内部へ不正侵入すること、外部から内部のサービスを妨害すること、内部の機密情報を外部へ持ち出すことなどがある

。このアクセス制御を担当する機器は、サービスを提供するサーバ自身や、このサーバへの通信を中継する中継装置（例えば、ルータ等）の、いずれかまたは両方である。

【0004】

従来のアクセス制御に関する先行文献として、特許文献1～3がある。

【0005】

また、代表的なネットワークプロトコルであるTCP/IPにおける帯域制御、IPSec、IPv6のFlow Labelに関する先行文献として、非特許文献1～3がある。

【0006】

（問題点1）P2P通信への対応

従来のアクセス制御では、基本的に、パケットを伝送するか破棄するかの、二者択一の制御が行われる。

【0007】

したがって、サーバが、完全に公開されているサービス、例えば、インターネットからのアクセス可能なWEBサービス等、を提供しているときには、このサーバへのパケットを、基本的に伝送するようにすればよい。

【0008】

一方、サーバが、固定的な範囲にアクセスが制限されるサービス、例えば、社内のネットワーク内にアクセスが限定されるファイル共有サービス等、を提供しているときには、この固定的な範囲外からのパケットを、全て破棄してしまえばよい。

【0009】

しかしながら、サーバが、出張等により社内から社外へ移動した社員が所有するコンピュータに対して、メールサービスを提供するような場合、以上のアクセス制御では対応できない。なぜなら、このような場合、社員が所有するコンピュータのアドレスやポート番号等は、社員が社内から社外へ移動すると、変更されてしまうからである。

【0010】

このような課題に対し、特許文献1～3では、いくつかの提案がなされている。ところが、これらによっても、P2P通信への対応が、不十分である。

【0011】

これらの文献では、内部から外部へパケットが伝送されると、パケットの伝送／破棄を判定する際、その逆向きのパケットを、伝送させるように、アクセス制御の判定条件を動的に変更している。これにより、外部と内部とで双方向の通信を行うこととしている。

【0012】

しかしながら、このような技術では、内部から外部へ向けてパケットが伝送されない限り、双方向の通信はできない。つまり、はじめに外部から内部へパケットを伝送してから双方向の通信を行おうとしても、それは不可能である。

【0013】

(問題点2) DOS攻撃に対する脆弱性

問題点1に対し、特定の条件を満たすパケットを、中継可能なように静的に判定条件を設定することも考えられる。しかしながら、現状のISP、ホットスポット等では、端末のアドレス等がDHCP等で動的に設定されるため、このような特定の条件を定めることは、事実上不可能に近い。

【0014】

また、このような設定を行うと、悪意を持つ者が、中継可能な条件を満たすパケットを偽造してサーバを攻撃する、DOS (Denial Of Service) の発生を防止できない。

【0015】

特許文献3では、DOS攻撃等の不正アクセスの対し、トラフィックシェーピングを用いて、使用帯域を制御している。しかしながら、不正アクセスによるパケットと、正当なアクセスパケットとが、混在して流れている場合、正当なアクセスによる通信の帯域を、不当に制限してしまう結果となるし、シェーピングの対象を、不正アクセスによるパケットのみに、限定することは、非常に難しい。

(問題点3) 暗号化への対応

従来のアクセス制御では、伝送／破棄の判定に、パケット内の情報を参照して

いる。ところが、第三者による盗聴を防ぐために、パケットを暗号化した場合、アクセス制御において、パケット内の情報が参照できないため、伝送／破棄の判定ができなくなってしまう。

【特許文献1】 特開平8-44642号公報

【特許文献2】 特表平10-504168号公報

【特許文献3】 特開2000-124955号公報

【非特許文献1】 文献名：「インターネットQoS」、共著：Paul Ferguson、Geott Huston、監訳：戸田巖、発行日：平成12年5月5日

【非特許文献2】 文献名：RFC2401 「IP Encapsulating Security Payload (ESP)」、共著：S. Kent、R. Atkinson、発行日：1998年11月

【非特許文献3】 文献名：RFC2460 「Internet Protocol, Version6 (IPv6) Specification」、共著：S. Deering、R. Hinden、発行日：1998年11月

【発明が解決しようとする課題】

そこで本発明は、より柔軟なアクセス制御を行え、パケットの暗号化に対応できる、アクセス制御方法及びその関連技術を提供することを目的とする。

【0016】

【課題を解決するための手段】

請求項1記載のアクセス制御方法は、外部ネットワークの端末から内部ネットワークのサーバへのアクセスを、外部ネットワークと内部ネットワークとを中継する中継装置を介して、制御するものであり、端末がサーバ宛に送出するパケットの伝送を、一定条件下で許容する第1ステップと、許容されたパケットに対し、サーバが接続を許可した場合、サーバ宛のパケット伝送の条件を変更する第2ステップと、しかる後、変更された条件で、端末とサーバとのパケット伝送を制御する第3ステップとを含む。

【0017】

この構成により、外部ネットワークの端末と、内部ネットワークのサーバとは

、廃棄の他、一定条件により制限された通信を行う状態と、この条件を緩めた条件下で、あるいは、さらに厳しくした条件下で、通信を行う状態との、少なくとも2つの伝送状態をとることができる。したがって、伝送／破棄という二者択一的なアクセス制御よりも、より柔軟なアクセス制御を行える。しかも、はじめに外部から内部へパケットを伝送してから双方向の通信を行える。

【 0 0 1 8 】

請求項 2 記載のアクセス制御方法では、第 1 ステップにおける一定条件は、端末からサーバ宛のパケット伝送の帯域を、一定範囲内とするものである。

【 0 0 1 9 】

この構成により、許容されたパケットに対し、サーバが接続を許可するまでの間、帯域の制限を加えることにより、万一不正アクセスによるパケットがサーバに到着しても、その量が制限されることになり、サーバを、不正アクセスから保護できる。

【 0 0 2 0 】

請求項 3 記載のアクセス制御方法では、第 1 ステップにおいて許容されるパケットは、サーバへ送信される認証情報を含む。

【 0 0 2 1 】

この構成により、一定条件が課される状態では、認証情報の伝送がなされることになり、認証情報で認証された端末のみ、変更された条件で、サーバにアクセスできるため、サーバを、不正アクセスから保護できる。

【 0 0 2 2 】

請求項 4 記載のアクセス制御方法では、第 2 ステップにおいて、端末とサーバとのそれぞれのアドレス及びポート番号に係る、フローについて、条件が変更される。

【 0 0 2 3 】

この構成により、該当するフローのみについて、他のフローとは区別して、アクセス制御できる。

【 0 0 2 4 】

請求項 5 記載のアクセス制御方法は、外部ネットワークの端末から内部ネット

ワークのサーバへのアクセスを、外部ネットワークと内部ネットワークとを中継する中継装置を介して、制御するものであり、端末から暗号化されたパケットが、サーバに到着した際、サーバは、この暗号化されたパケットを復号し、サーバは、中継装置に、この暗号化されたパケットに係る、アクセス制御に使用する情報を、中継装置へ通知する。

【0025】

この構成により、パケットが暗号化された状態では、中継装置が、アクセス制御に使用する、十分な情報を、得られない場合でも、中継装置は、サーバからの通知を利用して、正確なアクセス制御を実施できる。

【0026】

この情報は、例えば、中継装置が参照できない暗号化部分の情報（上位プロトコル種別、送受信ポート番号）、中継装置から参照可能な非暗号化部分の情報（IPv4のIDやIPv5/6のFlow-Label）の対応関係等である。

【0027】

請求項8記載のアクセス制御方法では、サーバと中継装置とのそれぞれにおいて、アクセス制御に使用する情報が保持され、サーバにおいて、この情報を変更した際、サーバは、その旨を中継装置へ通知する。

【0028】

この構成により、サーバが独自に情報を変更したような場合、サーバから中継装置へ通知がなされ、サーバと中継装置における、アクセス制御の整合性をとり、通信システム全体として、統一性のあるアクセス制御を実施できる。

【0029】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態を説明する。図1は、本発明の一実施の形態における通信システムの構成図、図2は同中継装置のブロック図、図5は同WEBサーバのブロック図である。

【0030】

図1に示すように、この通信システムは、中継装置6の上側に図示される外部ネットワーク7と、下側に図示される内部ネットワーク1とを有する。

【 0 0 3 1 】

内部ネットワーク 1 には、L A N ケーブル 2 が敷設され、L A N ケーブル 2 には、中継装置 6 の他、内部ネットワーク 1 に属する、W E B サーバ 3、社内メールサーバ 4、社内 D B サーバ 5 及びその他のクライアント端末（図示せず）が接続される。

【 0 0 3 2 】

中継装置 6 は、ネットワーク網 8 と L A N ケーブル 2 の両方に接続されている。

【 0 0 3 3 】

また、外部ネットワーク 7 には、ネットワーク網 8 があり、端末 9 は、W E B サーバ 3 による W E B サービスを受けることのみを許されている。一方、端末 1 0 は、内部ネットワーク 1 を利用する会社の社員が、出張先へ持参したコンピュータであり、端末 1 0 には、W E B サーバ 3 と、社内メールサーバ 4 によるサービスを受けることが許されている。

【 0 0 3 4 】

なお、社内 D B サーバ 5 のサービスは、内部ネットワーク 1 の内部のみで利用でき、内部ネットワーク 1 外のアクセスは禁止されている。

【 0 0 3 5 】

ここで、端末 9 が W E B サーバ 3 のサービスの利用を許可され、また、社内メールサーバ 4 のサービスの利用を禁止されるという、形態は、伝送／廃棄という二者択一的な、従来のアクセス制御で対応可能であるため、この点についての説明は省略する。

【 0 0 3 6 】

本発明で取り上げる問題は、社内メールサーバ 4 を不正アクセスから保護しながら、端末 1 0 に社内メールサーバ 4 を利用させることである。

【 0 0 3 7 】

次に、図 2 を用いて、中継装置 6 について詳しく説明する。まず、制御部 6 0 は、中継装置 6 の各構成要素を制御する。

【 0 0 3 8 】

通信部 61 は、外部ネットワーク 7 のネットワーク網 8 に接続される。また、通信部 62 は、内部ネットワーク 1 の LAN ケーブル 2 に接続される。

【0039】

記憶部 67 は、メモリなどの記憶媒体から構成される。そして、図 3 (a) に示すように、端末 10 の接続が許可される前の状態において、記憶部 67 は、通信部 61、62 を介して伝送されるパケットに係るフローを定義する情報（送信元についてのアドレス及びポート番号、宛先についてのアドレス及びポート番号）と、該当するフローについての帯域（本形態では、毎秒あたりのパケット数を用いる）の閾値 TH と、該当するフローについての帯域の測定値 V_n とを、フロー番号毎に、関連付けて記憶する。

【0040】

また、記憶部 67 には、接続を許可しうるフローが、予め定義されており、記憶部 67 に定義されたフローと全く関係ないフローは、不正アクセスとして、排除される。

【0041】

なお、記憶部 67 の内容の遷移は、簡単にまとめて言うと、記憶部 67 における帯域の閾値 TH は、内部ネットワーク 1 の社内メールサーバ 4 が、外部ネットワーク 7 の端末 10 からの接続を許可するまで、小さな値に設定され、社内メールサーバ 4 がこの接続を許可すると、より大きな値に変更されるものである。

【0042】

また、図 3 (a) に示すように、本形態では、フロー番号 1～4 の、合計 4 つのフローが定義されている。フロー番号 1 は、社内 DB サーバ 5 のサービスに関するものであり、外部ネットワーク 7 のどのアドレスからも、アクセスできない（閾値 $TH = 0$ ）ものである。

【0043】

フロー番号 2 は、内部ネットワーク 1 に属する端末（サーバ又はクライアント端末）から外部ネットワーク 7 へ出てゆくサービスに関するものであり、内部ネットワーク 1 のどのアドレスからアクセスしても、自由にアクセスできる（閾値 $TH = \infty$ ）ものである。

【0044】

フロー番号3は、WEBサーバ3のサービスに関するものであり、外部ネットワーク7のどのアドレスからアクセスしても、自由にアクセスできる（閾値 $TH = \infty$ ）ものである。

【0045】

フロー番号4は、社内メールサーバ4のサービスに関するものであり、外部ネットワーク7のどのアドレスからアクセスしても、一定条件下でアクセスできる（閾値 $TH = 10$ ）ものである。しかも、このアクセスは、プロトコル種別が、パスワード送信に関するPOPに限定される。

【0046】

後述するように、社内メールサーバ4にアクセスしようとする、端末10は、フロー番号4に従うパケットを、社内メールサーバ4に一定条件下で送信し、社内メールサーバ4が、その通信を許可する明示的なパケット（SYN-ACKフラグがオンになっているパケット）を発行した後に、この条件が大幅に緩和されるようになっている。

【0047】

図2において、分類部63は、記憶部67に記憶されたフローを定義する情報にしたがって、パケットのフローを分類する。

【0048】

測定部64は、分類されたフローについて帯域を測定し、測定値を、記憶部67において、該当するフロー番号の「測定値」のフィールドに格納する。

【0049】

判定部65は、分類されたフローについて、記憶部67に格納された帯域の測定値 V_n と閾値 TH とを大小比較し、 $V_n \leq TH$ であれば、伝送するという判定を下し、そうでなければ廃棄するという判定を下す。

【0050】

なお以下、説明を簡単にするために、判定部65は、「伝送する」という判定と、「廃棄する」という判定との、2種類の判定のみをなすものとする。しかし、廃棄はしないが伝送を遅らせたり、パケットの優先度を変更したりする判定を

下すようにすることもでき、このようにしても、本発明に包含される。

【0051】

帯域制御部 66 には、判定部 65 により伝送すると判定されたパケットが、セットされ、帯域制御部 66 は、その帯域制御のルールに従って、パケットを帯域制御部 66 自体において廃棄しない限り、通信部 61、62 から順次送信する。

【0052】

本形態の帯域制御部 66 における帯域制御方式は、任意である。例えば、FIFO、RED、RIO 等のキューイング、PQ、WRR 等のスケジューラ等を自由に選択して使用できる。

【0053】

次に、図 5 を用いて、社内メールサーバ 4 について詳しく説明する。まず、制御部 40 は、社内メールサーバ 4 の各構成要素を制御する。通信部 41 は、LAN ケーブル 2 に接続される。

【0054】

記憶部 48 は、メモリなどの記憶媒体から構成され、中継装置 6 の記憶部 67 と同様の内容を持つ。但し、一時的に、記憶部 48 の内容と、記憶部 67 の内容が、一致しなくなることがあるが、この情報の不整合は、後述する変更通知により、直ちに解消されるようになっている。勿論、記憶部 48 の遷移は、記憶部 67 の遷移と基本的に同じである。

【0055】

アプリケーション部 42 は、社内メールサーバ 4 としての機能を実現するための、(メールサービス) アプリケーションを実行するものである。

【0056】

暗号処理部 43 は、暗号化されたパケットを復号する。この暗号化されたパケットに係る、アクセス制御に使用する情報は、通信部 41 を介して、中継装置 6 へ通知される。

【0057】

ここで、IPsec 等により暗号化されたパケットでは、アクセス制御において、パケットを分類するために必要な情報までが、暗号化されてしまう。その

ため、パケットの分類が、不完全になる。アクセス制御で必要となる情報は、暗号化されたパケットを復号できる、送信元または宛先の社内メールサーバ4でしか取得できない。

【0058】

TCP/IPのバージョン6のIPでは、このような暗号化されたパケットが複数混在した場合にも、パケットを分類可能とするためにフローラベルが導入されている。しかしながら、フローラベルから暗号化されている送受信ポート番号等との関係を判定できるのは、送受信端末のみである。

【0059】

そこで、本形態では、社内メールサーバ4に暗号処理部43を設け、復号したパケットから、アクセス制御の分類に必要な情報が得られたら、これを、社内メールサーバ4のみで持つのではなく、中継装置6に通知し、中継装置6の分類処理と、社内メールサーバ4の分類処理の整合性を確保している。

【0060】

図5において、分類部44、測定部45、判定部46、帯域制御部47は、図2の分類部63、測定部64、判定部65、帯域制御部66と、同様のものである。

【0061】

即ち、分類部44は、記憶部48に記憶されたフローを定義する情報にしたがって、パケットのフローを分類する。

【0062】

測定部45は、分類されたフローについて帯域を測定し、測定値を、記憶部48において、該当するフロー番号の「測定値」のフィールドに格納する。

【0063】

判定部46は、分類されたフローについて、記憶部48に格納された帯域の測定値 V_n と閾値 TH とを大小比較し、 $V_n \leq TH$ であれば、伝送するという判定を下し、そうでなければ廃棄するという判定を下す。

【0064】

帯域制御部47には、判定部45により伝送すると判定されたパケットが、セ

ットされ、帯域制御部 4 7 は、その帯域制御のルールに従って、パケットを帯域制御部 4 7 自体において廃棄しない限り、通信部 4 1 から順次送信する。

【 0 0 6 5 】

本形態の帯域制御部 4 7 における帯域制御方式は、任意である。例えば、F I F O、R E D、R I O等のキューイング、P Q、W R R等のスケジューラ等を自由に選択して使用できる。

【 0 0 6 6 】

(変更通知)

さて、パケット交換の通信においては、接続要求とそれに対する明示的な接続許可を通知するコネクション型通信と、接続要求とそれに対する明示的な接続許可を通知しないコネクションレス型通信の二つの方式がある。

【 0 0 6 7 】

現在最も普及しているインターネットの通信プロトコルである T C P / I P においては、コネクション型通信として T C P が、コネクションレス型通信には U D P がある。

【 0 0 6 8 】

また T C P および U D P では、一組の端末（この端末には、サーバを含む。）間で複数の通信を独立して行えるように、端末は、通信毎にポート番号を割当てる。

【 0 0 6 9 】

したがって、中継装置 6 の分類部 6 3 は、送受信アドレスと送受信ポート、そして T C P か U D P かを示す上位プロトコル種別を参照することで、複数の通信を分類可能となる。

【 0 0 7 0 】

コネクション型通信である T C P では、接続を要求するパケット（T C P フラグ内の S Y N フラグがオンになっているパケット）を受信した社内メールサーバ 4 は、接続を許可する場合には接続を許可するパケット（S Y N - A C K フラグがオンになっているパケットや A C K フラグがオンとなっているパケット）を送信する。

【 0 0 7 1 】

一方、社内メールサーバ 4 は、接続を許可しない場合、接続を許可しないこと示すパケット（TCP フラグ内の FIN フラグがオンとなっているパケット）を送信する。

【 0 0 7 2 】

TCP/IP において、接続を許可しないことを明示的に示すには、TCP の FIN パケット以外に、ICMP の Destination Unreachable を応答することによってもよい。これは、TCP および UDP に共通で利用可能である。

【 0 0 7 3 】

なお、接続を要求するパケットや、接続を許可する／許可しないといった明示的なパケットを、送受信しないコネクションレス型通信である、UDP においては、送受信アドレスおよび送受信ポート番号の組み合わせが一致するパケットをの送受信をトリガにするとよい。

【 0 0 7 4 】

コネクションレス型通信においては、接続の要求・接続の許可・接続の不許可を明示するパケットの送受信が行われないため、アクセス制御の判定が正確でなくなる可能性がある。

【 0 0 7 5 】

本形態では、社内メールサーバ 4 が、中継装置 6 の意向とは無関係に、端末 1 0 へ明示的な接続の許可を行った場合、社内メールサーバ 4 から中継装置 6 へ変更通知を発行して、中継装置 6 上の記憶部 6 7 を、社内メールサーバ 4 の記憶部 4 8 と一致させることにしている。

【 0 0 7 6 】

この通知をうまく利用すれば、中継装置 6 でアクセス制御に関する全ての情報を保持しなかった従来の方式に対し、アクセス制御に関する情報を、中継装置 6 と社内メールサーバ 4 とで、分散して保持することもできるようになる。中継装置 6 上の情報の量及び処理負担を削減できる。また中継装置 6 では、実際には既に通信されなくなったフローに関する情報を保持しなくても足りるよ

うになるから、一層処理負担を軽減できる。

【 0 0 7 7 】

また、この変更通知により、社内メールサーバ 4 の帯域制御の処理内容と、中継装置 6 の帯域制御の処理内容の整合性を、確保できる。

【 0 0 7 8 】

これにより、社内メールサーバ 4 から中継装置 6 へ届いたパケットが、帯域不足のために、中継装置 6 で破棄されたり、逆に、中継装置 6 から外向きの帯域が必要以上に確保されて、他のフローが要する帯域が圧迫されるような事態を、回避できる。

【 0 0 7 9 】

(帯域制御)

パケット交換ネットワークでは、その仕組みの制約上、パケットの送信側でしか帯域制御が行えない。

【 0 0 8 0 】

従って、社内メールサーバ 4 から中継装置 6 へのパケットに関しては、社内メールサーバ 4 側でしか帯域制御を行えず、中継装置 6 から社内メールサーバ 4 へのパケットに関しては、中継装置 6 側でしか帯域制御を行えない。

【 0 0 8 1 】

そこで、本形態では、外部からの不正なアクセスに対する応答によって、社内メールサーバ 4 の帯域を不正使用されることを防ぐため、帯域制御部を、中継装置 6 と社内メールサーバ 4 の両方に設けている。

【 0 0 8 2 】

次に、図 4 を参照しながら、中継装置 6 の動作を説明する。まず、ステップ 1 にて、制御部 6 0 は、通信部 6 1 または通信部 6 2 にパケットが到着するのを待つ。

【 0 0 8 3 】

到着したら、ステップ 2 にて、このパケットが、社内メールサーバ 4 からの変更通知でないかどうかチェックする。もしそうなら、制御部 6 0 は、ステップ 3 にて、変更通知のとおり、記憶部 6 7 の内容を更新する。これにより、記憶部 6

7の内容と、記憶部48の内容の整合性が担保される。

【0084】

変更通知でなければ、ステップ4にて、制御部60は、分類部63に分類を命ずる。すると、分類部63は、このパケットに該当するフローが、記憶部67に存在するかどうかチェックする。

【0085】

存在すれば、ステップ5にて、分類部63は、そのフローの各値（送信元及び宛先に関するアドレス及びポート番号等）が確定しているかどうかチェックする。因みに、分類部63は、図3に矢印で示しているように、フロー番号が大きいものの順に、検討を行う。ここで、確定していない場合とは、図3に「*」で示したように、値が未定の場合である。

【0086】

確定していなければ、分類部63は、ステップ6にて、新しいエントリ（フロー番号は、現在最大のものに「1」を足した番号となる）を追加し、パケットから得られた各値（送信元及び宛先に関するアドレス及びポート番号等）をセットして、ステップ7へ処理を移す。確定していれば、新たなフローを追加する必要はないので、分類部63は、ステップ5からステップ7へ処理を移す。

【0087】

ステップ4にて、該当フローがなければ、これは不正アクセスの可能性があるため、分類部63は、分類を中止してその旨制御部60に報告する。この報告を受けた制御部60は、即座にステップ10へ処理を移し、このパケットを廃棄する。

【0088】

さて、ステップ7では、測定部64が該当フローの伝送速度を測定し、その測定値 V_n が、該当フローの測定値のフィールドにセットされる。

【0089】

次に、ステップ8では、判定部65が、該当フローの測定値 V_n と閾値 TH とを、大小比較し、判定部65は、 $V_n \leq TH$ であれば「伝送する」と判定し、パケットが帯域制御部66に出力される。この後、帯域制御部66は、その帯域制

御方式に従って、パケットを自身で廃棄しない限り、順次、通信部 6 1 または通信部 6 2 から出力する。

【 0 0 9 0 】

一方、そうでなければ、判定部 6 5 は、「廃棄する」と判定し、パケットは帯域制御部 6 6 に出力されることなく、廃棄される。

【 0 0 9 1 】

そして、ステップ 1 以降の処理が、処理が終了するまで繰り返される（ステップ 1 1）。

【 0 0 9 2 】

次に、図 6 を用いて、社内メールサーバ 4 の動作を説明する。まず、ステップ 3 1 にて、制御部 4 0 は、変更フラグに初期値としての「OFF」をセットする。このフラグは、社内メールサーバ 4 がそれ自身の判断で、記憶部 4 8 の内容を変更したかどうかを示すフラグであり、「ON」なら変更したことを、「OFF」なら変更していないことを表す。そして、「ON」なら記憶部 4 8 の内容と、記憶部 6 7 の内容に相違があることになるので、しかるべきタイミング（ステップ 4 6）で、中継装置 6 へ変更通知を発行することとしている。

【 0 0 9 3 】

さてステップ 3 2 にて、制御部 4 0 は、通信部 4 1 にパケットが到着するのを待つ。到着するまでは、ステップ 3 3 にて、制御部 4 0 は、アプリケーション部 4 2 による処理を実施する。

【 0 0 9 4 】

到着したら、ステップ 3 4 にて、このパケットが、暗号化されたものでないかどうかチェックする。もしそうなら、制御部 4 0 は、ステップ 3 5 にて、暗号処理部 4 3 にこのパケットを復号させてから、ステップ 3 6 へ処理を移す。暗号化されていなければ、制御部 4 0 は、ステップ 3 4 からステップ 3 6 へ処理を移す。

【 0 0 9 5 】

次に、ステップ 3 6 にて、制御部 4 0 は、分類部 4 4 に分類を命ずる。すると、分類部 4 4 は、このパケットに該当するフローが、記憶部 4 8 に存在するかど

うかチェックする。

【0096】

存在すれば、ステップ37にて、分類部44は、そのフローの各値（送信元及び宛先に関するアドレス及びポート番号等）が確定しているかどうかチェックする。因みに、分類部44も、分類部63と同様に、図3に矢印で示しているように、フロー番号が大きいものの順に、検討を行う。ここで、確定していない場合とは、図3に「*」で示したように、値が未定の場合である。

【0097】

確定していなければ、分類部44は、ステップ38にて、新しいエントリ（フロー番号は、現在最大のものに「1」を足した番号となる）を追加し、パケットから得られた各値（送信元及び宛先に関するアドレス及びポート番号等）をセットする。また、これにより、記憶部48が記憶部67と一致しなくなった可能性があるため、変更フラグを「ON」とする。

【0098】

そして、ステップ39へ処理を移す。ステップ39では、分類部44は、端末10に接続を許可するSYN-ACKのフラグをオンにしたパケットを、送信するかどうか、制御部40に確認する。送信するのなら、該当フローの一定条件を緩和するため、ステップ40にて、記憶部48において、該当フローの閾値THに、 ∞ （自由に通信を認める）の値をセットし、ステップ41へ処理を移す。送信しないなら、分類部44は、ステップ39からステップ41へ処理を移る。

【0099】

さて、ステップ37にて、値が確定していれば、新たなフローを追加する必要はないので、分類部44は、ステップ37からステップ41へ処理を移す。

【0100】

ステップ36にて、該当フローがなければ、これは不正アクセスの可能性があるため、分類部44は、分類を中止してその旨制御部40に報告する。この報告を受けた制御部40は、即座にステップ44へ処理を移し、このパケットを廃棄する。

【0101】

さて、ステップ 4 1 では、測定部 4 5 が該当フローの伝送速度を測定し、その測定値 V_n が、該当フローの測定値のフィールドにセットされる。

【0102】

次に、ステップ 4 2 では、判定部 4 6 が、該当フローの測定値 V_n と閾値 TH とを、大小比較し、判定部 4 6 は、 $V_n \leq TH$ であれば「伝送する」と判定し、パケットが帯域制御部 4 7 に出力される。この後、帯域制御部 4 7 は、その帯域制御方式に従って、パケットを自身で廃棄しない限り、順次、通信部 4 1 から出力する。

【0103】

一方、そうでなければ、判定部 4 6 は、「廃棄する」と判定し、パケットは帯域制御部 4 7 に出力されることなく、廃棄される。

【0104】

そして、ステップ 3 2 以降の処理が、処理が終了するまで繰り返される（ステップ 4 8）。

【0105】

次に、図 7、図 3 を用いて、端末 1 0 が一定条件下で社内メールサーバ 4 との接続要求をするための通信を開始し、それが認められ、条件が緩和され、通信が円滑に行われるまでの処理の流れを説明する。

【0106】

まず、図 7 の時刻 t_1 において、端末 1 0 が、社内メールサーバ 4 に SYN フラグがオンとなったパケット（アカウント、パスワード等の認証情報を含む情報）を、POP プロトコルにしたがい送信する。このとき、記憶部 4 8、記憶部 6 7 の内容は、図 3（a）に示すとおりである。

【0107】

このパケットは、フロー番号 4 に属するものであるため、このフローの測定値 V_4 が閾値 TH 以下であるとき、通信が許可される。

【0108】

ところが、時刻 t_1 前後では、測定値 V_4 が閾値 TH を超えていたため、通信は失敗し、時刻 t_2 において、社内メールサーバ 4 から端末 1 0 へ FIN フラグ

がオンになったパケットが返される。

【0109】

そこで、端末10は、パケットの伝送速度を下げて、時刻 t_3 にて、再度、SYNフラグをオンにしたパケットを、社内メールサーバ4へ送信する。すると、上記一定条件が満たされて、時刻 t_4 において、社内メールサーバ4から端末10へ接続を許可するパケット（SYN-ACKフラグがオンになったパケット）が返される。

【0110】

このとき、記憶部48の内容は、一旦、図3（b）に示すように、変化する。即ち、フロー番号4の内容を、複写した新たなエントリ（フロー番号5）が作成され、端末10のアドレス及びポート番号等の各値がセットされる。

【0111】

さらに、図3（c）に示すように、接続を許可したフロー番号について、閾値THが10から ∞ に拡大され、条件が緩和される。そして、この変更は、社内メールサーバ4から中継装置6へ変更通知により知らされ、記憶部67の内容も、図3（c）の内容と一致する。

【0112】

しかるのち、時刻 t_5 以降において、広い帯域による円滑な通信が実行される。

【0113】

さらに、時刻 t_9 において、端末10は、今度は、メールサービスそのものを受けるため、社内メールサーバ4にSYNフラグがオンとなったパケット（パスワードを含む情報）を、MAILプロトコルにしたがい送信する。

【0114】

すると、図3（d）に示すように、社内メールサーバ4が、新たなエントリ（フロー番号6）を追加し、MAILプロトコルによる通信が実行される。勿論、このときの記憶部48の変更は、直ちに、中継装置6へ通知され、記憶部48の変更内容は、すぐに記憶部67に反映される。

【0115】

【発明の効果】

本発明によれば、伝送／破棄といった二者択一的なアクセス制御ではなく、他の正当なアクセスの通信に支障のないように制御された帯域の範囲内において、より柔軟なアクセス制御を行える。

【0 1 1 6】

また、内部ネットワークのサーバから、中継装置へ通知を行うことにより、従来のアクセス制御では、正確な判定が困難であったコネクションレス型通信や暗号化された通信に対しても、アクセス制御に関する判定を、正確に実施できる。

【図面の簡単な説明】**【図 1】**

本発明の一実施の形態における通信システムの構成図

【図 2】

同中継装置のブロック図

【図 3】

(a) 同記憶部の遷移説明図

(b) 同記憶部の遷移説明図

(c) 同記憶部の遷移説明図

(d) 同記憶部の遷移説明図

【図 4】

同中継装置のフローチャート

【図 5】

同サーバのブロック図

【図 6】

同サーバのフローチャート

【図 7】

同パケット伝送を示すタイムチャート

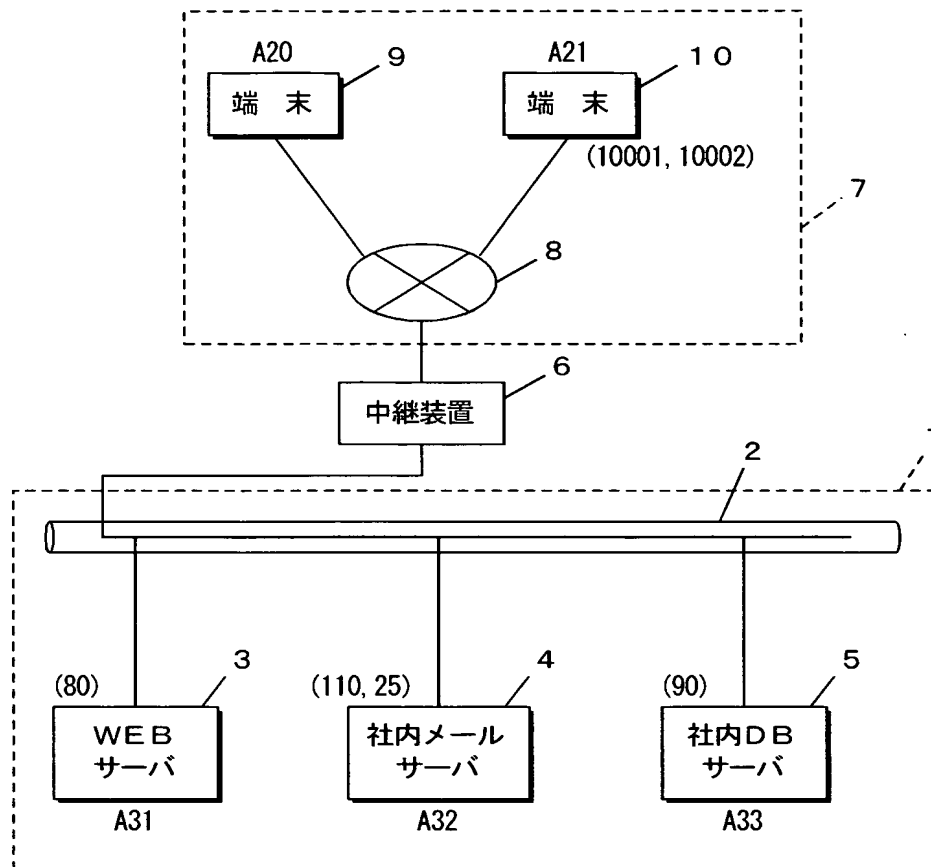
【符号の説明】

- 1 内部ネットワーク
- 2 LAN ケーブル

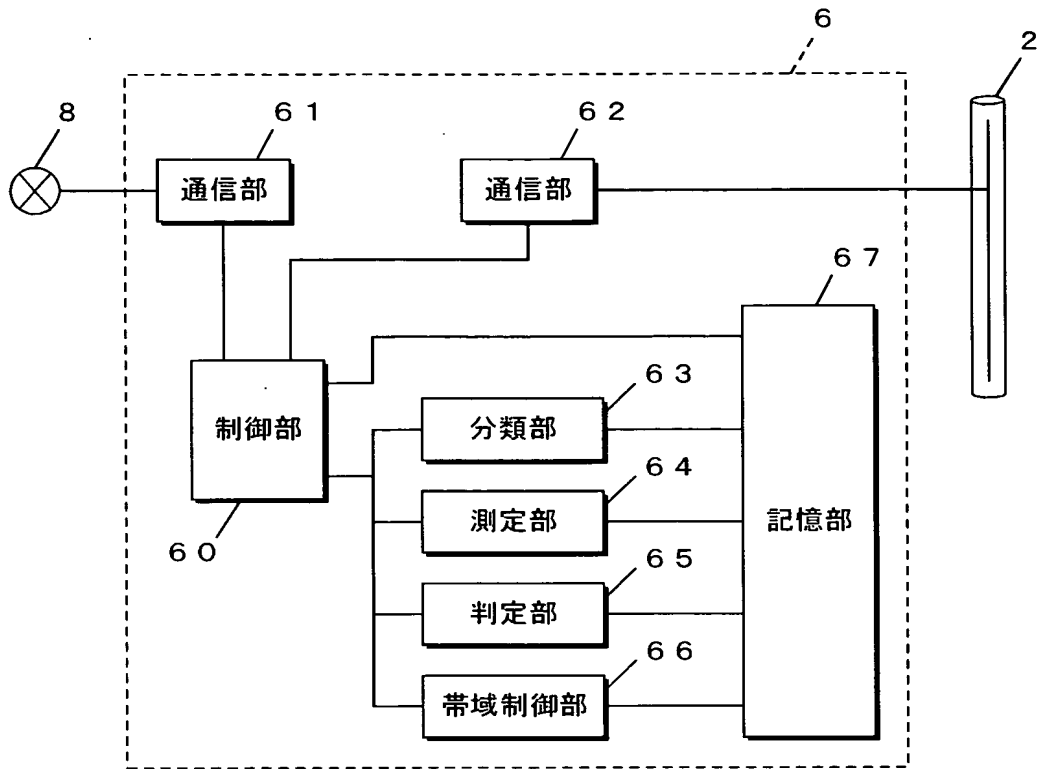
- 3 WEBサーバ
- 4 社内メールサーバ
- 5 社内DBサーバ
- 6 中継装置
- 7 外部ネットワーク
- 8 ネットワーク網
- 9、10 端末
- 40、60 制御部
- 41、61、62 通信部
- 42 アプリケーション部
- 43 暗号処理部
- 44、63 分類部
- 45、64 測定部
- 46、65 判定部
- 47、66 帯域制御部
- 48、67 記憶部

【書類名】 図面

【図 1】



【図 2】



【図 3】

(a) *は任意

フロー 番号	送 信 元		宛 先		閾値 TH (パケット数/s)	測定値 (パケット数/s)	
	アドレス	ポート 番号	アドレス	ポート 番号			
1	外部NW	*	内部NW	*	0	V1	t1~t3
2	内部NW	*	外部NW	*	∞	V2	
3	*	*	A31	80 (HTTP)	∞	V3	
4	*	*	A32	110 (POP)	10	V4	

(b)

4	*	*	A32	110 (POP)	10	V4	t4
5	A21	10001	A32	110 (POP)	10	V5	

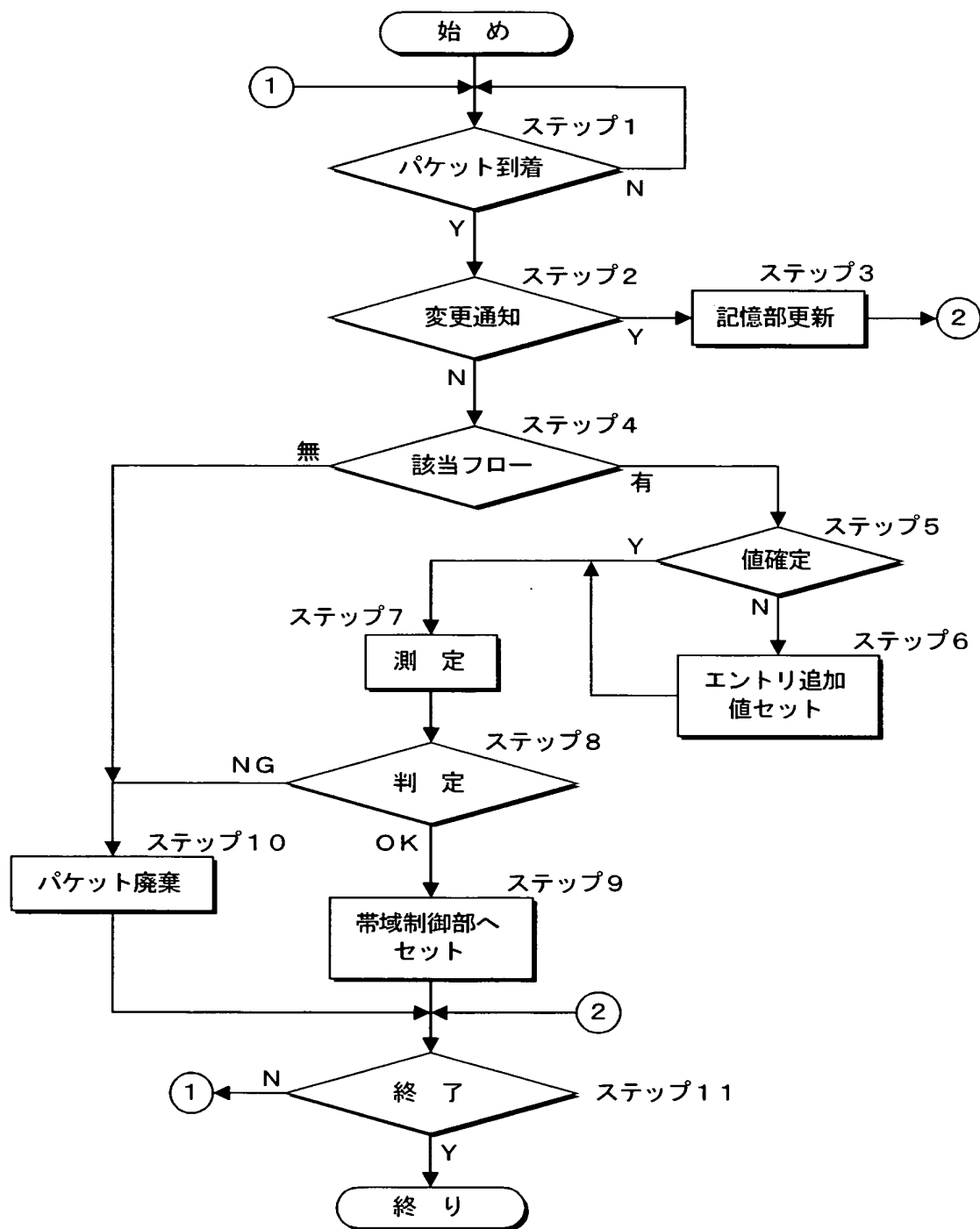
(c)

4	*	*	A32	110 (POP)	10	V4	t4
5	A21	10001	A32	110 (POP)	∞	V5	

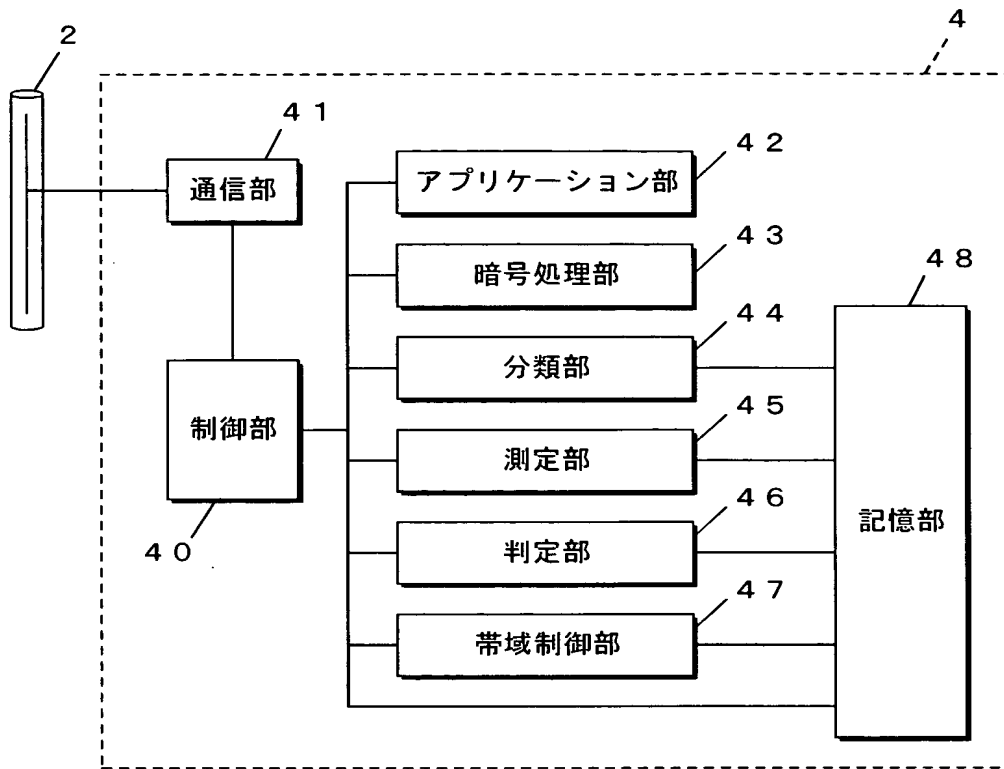
(d)

4	*	*	A32	110 (POP)	10	V4	t10
5	A21	10001	A32	110 (POP)	∞	V5	
6	A21	10002	A32	25 (MAIL)	∞	V6	

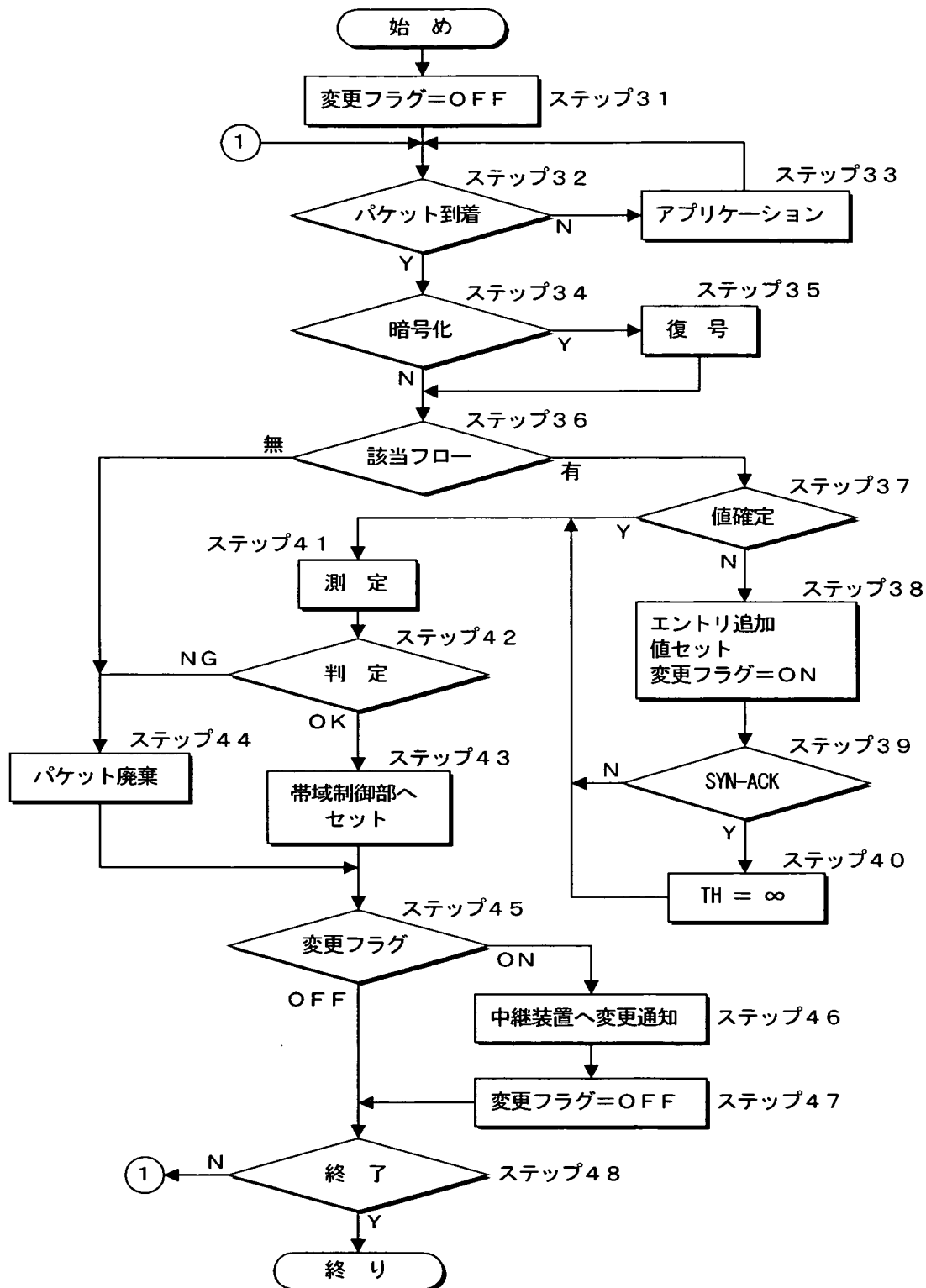
【図4】



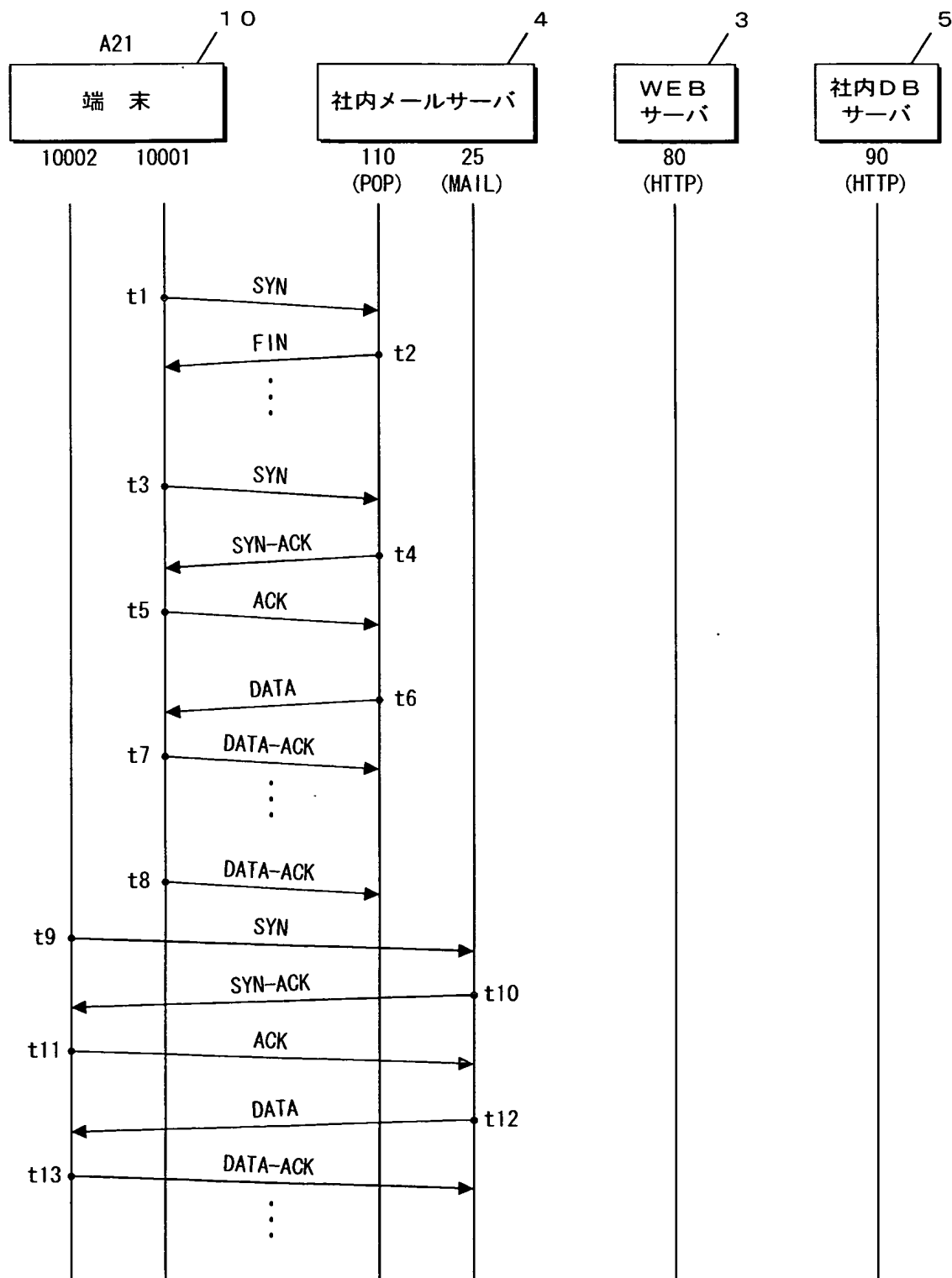
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 より柔軟なアクセス制御を行え、パケットの暗号化に対応できるアクセス制御方法を提供する。

【解決手段】 外部ネットワーク 7 の端末 1 0 から内部ネットワーク 1 のサーバ 4 へのアクセスを中継装置 6 を介して、制御する。中継装置及びサーバでは、端末がサーバ宛に送出するパケットの伝送を、一定条件下で許容する。許容されたパケットに対し、サーバが接続を許可した場合、サーバ宛のパケット伝送の条件を緩和する。しかる後、緩和された条件で、端末とサーバとのパケット伝送を制御する。暗号化については、サーバで復号し、中継装置に通知を行う。

【選択図】 図 1

特願 2 0 0 3 - 1 0 3 7 6 0

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社